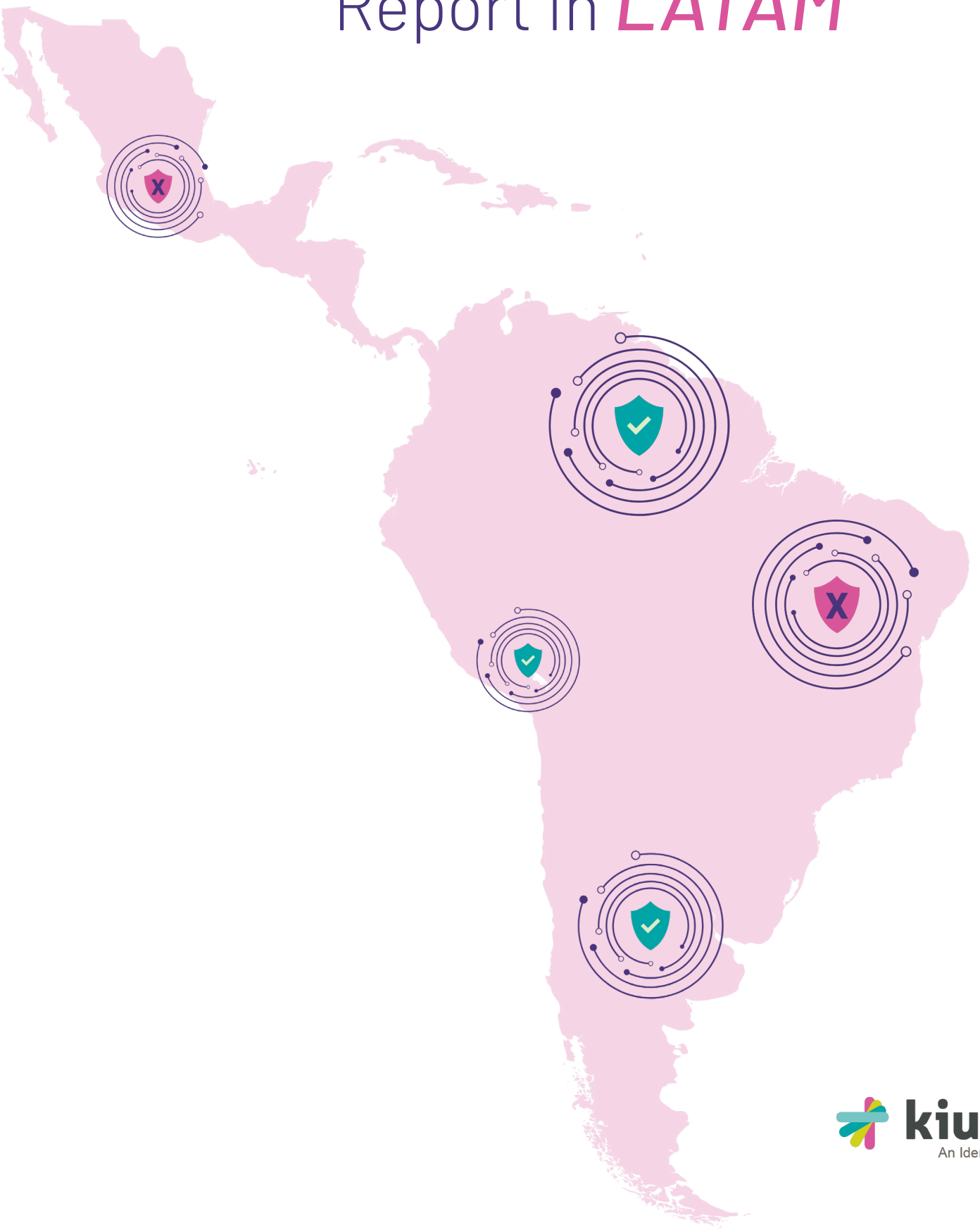
Software Security
Report in *LATAM*



kiuwan
An Idera, Inc. Company

INDEX

Overview.....1

The State of AppSec in LATAM.....2

Top 10 AppSec Trends in South America.....2

How Organizations Are Reacting to Address Risks.....7

How LATAM Organizations Can Prepare for the Future.....8

Secure Your Organization's Application Development.....10

Overview:

The last few years have seen South American (LATAM) countries become a hub for technology startups and established organizations to expand. These countries have become attractive because of low development costs, access to large talent pools, and a large potential market.

However, while LATAM countries have been quick to adopt the development of applications and software systems, cybersecurity has yet to catch up. This lack of security has become a significant threat to the development of applications and software systems, not to mention a major hindrance to the success of companies that have invested in LATAM.

*...**Brazil**, 16th on the list at USD **$ 1.38 million**, saw the **largest relative cost increase** of a data breach, up USD 0.3 million or 27.8%...*

IBM Cost of a Data Breach Report 2022

While numerous LATAM AppSec Reports have detailed just how much of an issue this is, only a few reports have gone in-depth on the specific issues associated with cybersecurity in LATAM and how to deal with them. This is why Kiuwan conducted a comprehensive analysis of the LATAM cybersecurity landscape.

This LATAM AppSec Report seeks to fill that gap by providing an in-depth look at the cybersecurity landscape in LATAM countries. It will discuss the current state of AppSec, highlight common issues, and suggest ways to improve application security in these countries. The report will also discuss the current cyber threats that LATAM companies face and provide best practices for mitigating these threats. In doing so, this report will provide organizations with the information they need to make informed decisions regarding their LATAM cybersecurity strategy.

The State of AppSec in *LATAM*

A report by Check Point Research revealed that while organizations worldwide experienced an increase in cyber attacks in 2022, LATAM countries experienced a drastic increase. For instance, on average, there were 1,662 attacks on each organization in Latin America in the first six months of 2022, compared to an average of 722 attacks per organization. This indicates that not only are LATAM companies more likely to be targeted, but they are also less prepared to handle these attacks.

*1st half of 2022

1,662 Attacks

*Average Cyber Attack per Organization

722 Attacks

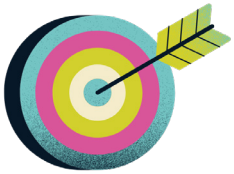
In an interview with CyberTalk.org, Francisco Robayo, a cybersecurity expert in the LATAM region, pointed out that while the LATAM region has great potential for application development, the volatile nature of the region's political and social climate makes it challenging to keep up with cybersecurity development. Moreover, he indicated that most LATAM entities (and government entities) have yet to modify their organizational culture to make cybersecurity chief among all other priorities.

It is also worth mentioning that while the world makes progress in application security by having regulations and laws that protect data, such as the GDPR (General Data Protection Regulation), LATAM countries still need to catch up in this aspect. Moreover, even when LATAM countries manage to establish regulations, they are often ignored.

Top 10 *AppSec* Trends in South America

Looking at LATAM countries individually, it is evident that each one has its own cybersecurity challenges and trends. However, there are some common trends similar across this region. Here are the top 10 AppSec trends that this LATAM AppSec Report found:

1. LATAM Governments Were *Prime Targets for Ransomware Attacks*



While there were numerous ransomware attacks on LATAM companies in 2022, LATAM governments were the most targeted. The attacks exposed most government systems vulnerabilities, such as failing to keep software updated with critical patches. Nevertheless, these attacks allowed organizations to improve their cybersecurity practices. Some of the worst attacks were:

Costa Rica – *Conti Group Attack*

In April 2022, Conti, a Russian-aligned hacking group, attacked Costa Rica's government systems, crippling some essential government services for nearly a month. The malicious attack had a detrimental impact on the Ministry of Finance's TIC and Virtual Tax Administration systems, which are pivotal for collecting taxes and paying salaries. This led to the government switching to paper-based processes until they could restore the systems.

Due to the length of the attack, the Costa Rican government declared it a national emergency in May after another attack targeted the country's social security fund. This event highlighted the gaps in public cybersecurity infrastructure and the need for LATAM countries to take a more proactive approach regarding application security.

Chile – *Multiple Ransomware Attacks*

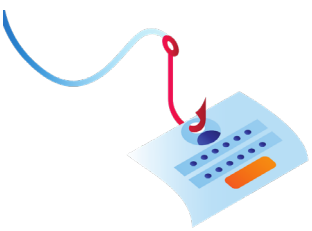
2022 was also a tumultuous year for Chile as ransomware attacks crippled the country. In September 2022, hackers attacked over 150 computers used by the Chilean judiciary system, which led to the paralysis of several functions. This attack was only a few weeks after another massive email leak from the Chilean Armed Forces that exploited an old and known vulnerability. Later, the National Consumer Service also experienced an attack on its computer systems, leading to outages on its remote service system.

Dominican Republic – *Quantum Ransomware Attack*

In August 2022, hackers demanded a ransom of $650,000 after they infected the systems at the Dominican Republic's Ministry of Agriculture. This led to one of the most significant data breaches in the country, as hackers claimed to have stolen over 1 Tb of files.

Unique to this attack was the hacker's use of a modified version of Quantum Ransomware — a ransomware strain that the LATAM region had not seen before. The attack, which targeted Dominican Agrarian Institute (IAD) servers and databases, had a detrimental effect on the IAD's ability to communicate with farmers, who often rely on government aid from the IAD.

2. *Spear-Phishing Attacks* Continue to Grow



Phishing attacks have long been among the most common cyber threats across LATAM countries for years. 2022 showed the same trend as the number of phishing attacks and ransomware variants increased significantly. In fact, LATAM countries continued to be the primary target for spear-phishing attacks. This strategy tricks internet users into giving away personal information through emails and instant messages which appear legitimate. Yet, the most menacing scheme of spear phishing is when criminals specifically target an organization or company to access confidential data.


&


In 2022, Spain and Mexico were on high alert after it emerged that phishing attacks using a banking Trojan named Grandoreiro had infiltrated LATAM countries. The threat was particularly concerning due to the nature of the Trojan, which can infect computers and steal banking credentials, passwords, and financial information. In Spain, hackers used the Trojan to impersonate the Public Ministry of Spain through emails and infect computers when unsuspecting users opened the emails leading to significant data breaches. In Mexico, hackers used the same Trojan to send phishing emails impersonating the Attorney General's Office of Mexico City.

3. *Hacktivism* Continues to Be a Growing Trend

Hacktivism is when hackers break into computer systems for political or social causes. LATAM countries are particularly vulnerable to hacktivism as the region has a long history of political and civil unrest. LATAM countries were no strangers to hacktivism in 2022, as hackers attacked numerous organizations demanding political or social change.

Guacamaya, a popular hacktivist group in Latin America, was especially active in 2022. In September, the group hacked several military and police agencies in ***Colombia, El Salvador, Peru, Chile, and Mexico*** in an attempt to highlight the abuses carried out by these agencies. The group released over 10 Tb of classified data stolen from the organizations and posted messages on their website demanding justice for victims of state-sponsored violence.

4. *Botnet Campaigns Still Active* in Latin American Countries

Botnets are networks of computers that are infected with malicious code, allowing hackers to control all of the computers in the network and use them to launch distributed denial-of-service (DDoS) attacks. The most common botnet attack seen in LATAM countries is the "***zombie*" *attack***, which infects computers with malicious code that turns them into "zombies" or bots that hackers can use to launch coordinated attacks on specific targets.

Botnet campaigns such as Bladabindi, Mirai, and Gh0st are still the most used attack methods in LATAM countries. As revealed by Fortinet, a cybersecurity corporation, the Mirai botnet alone is responsible for over 80 percent of all Botnet attacks in LATAM countries. This region is particularly vulnerable to these attacks since there isn't a consistent patching policy within most LATAM governments and private companies. This leaves systems and networks vulnerable to attack.

5. LATAM Now, a *Hotspot for Cryptojacking* Campaigns

Cryptojacking is an attack where malicious actors use a victim's computer or network to mine cryptocurrency without the user's permission. LATAM countries have become hotspots for cryptojacking campaigns in the past few years. In a report by SonicWall, a cybersecurity firm, Mexico emerged as the most targeted LATAM country in only the first half of 2022. The report also revealed that the number of cryptojacking cases in the LATAM financial section grew by 269 percent in only the first half of 2022, highlighting LATAM countries' vulnerability to this attack.

6. *Threats Related to Remote Working* on the Rise

2020 saw LATAM companies scrambling to shift their operations to remote work in response to the COVID-19 pandemic. LATAM countries have seen a dramatic increase in remote working since then as the standard of work continues to shift. Not only were businesses faced with operational issues, but they also had to contend with security threats. With the transition to remote work, employees relied heavily on email communication, applications, and platforms, exposing their respective organizations' networks to cybercrime risks.

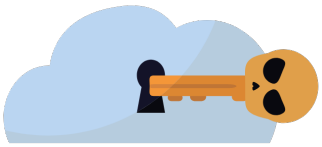
Risks such as malware attacks, phishing attempts, ransomware campaigns, and data theft became more prevalent as LATAM organizations scrambled to keep up with the transition. A 2022 report released by KPMG revealed that 86 percent of all surveyed companies in LATAM reported that remote working negatively affected cybersecurity and fraud prevention programs at their company.

7. *Homegrown Malware* Growing in Popularity

Malware is software designed to gain access to or damage a computer, server, or network without the user's knowledge or consent. Homegrown malware is a software developed by malicious actors within the country or region they intend to use. This type of malware is becoming increasingly popular among cybercriminals in Latin America as it is more difficult to detect and has a better chance of targeting organizations in the region. Criminals utilize homegrown malware to target banks, governments, and other high-profile institutions.

In 2022, Statista reported that the number of cybersecurity incidents caused by homegrown malware in LATAM had risen in the second quarter of 2022. Cuba, Venezuela, Nicaragua, and Bolivia were some of the countries that experienced the highest number of homegrown malware incidents.

8. Growing Number of *Cloud Vulnerabilities*



Cloud computing is becoming increasingly popular among LATAM companies and organizations, with nearly 80 percent of businesses in the region now using cloud-based solutions. However, as more organizations move to the cloud, they become exposed to many cloud-related risks, such as data theft, malicious insiders, and application vulnerabilities.

The LATAM region saw an alarming increase in cloud vulnerabilities in 2022, with many cloud-related threats leveraged to launch cyber-attacks.

9. *Slow Responses* and Insufficient Concern Over Application Security

As application security becomes increasingly important, it is necessary for organizations in the LATAM region to take steps toward strengthening application security. However, many LATAM organizations see application security as an afterthought, which is a cause for concern. Many organizations in the region lack application security best practices, such as application hardening and testing. As a result, application vulnerabilities are often unchecked, leaving it open to attacks from malicious actors.

A case in point is the numerous attacks in 2022 where affected entities did not address application vulnerabilities, leaving the application open to attacks. For instance, the Chilean Armed Forces' ransomware attack resulted from an application vulnerability that was left unchecked over a long period.

10. Increase in *Insider Threats*

Insider threats refer to cybersecurity threats that originate from within an organization. They pose a significant concern for organizations in the LATAM region, as malicious actors can use privileged access to the organization's systems, networks, and data to launch attacks.

In 2022, there was a significant increase in insider threats in LATAM countries. This could be attributed to the rise in remote working, which gave malicious actors easier access to an organization's systems and data. For instance, in Chile, a malicious insider incident in an ongoing case saw a Judiciary official adulterate a case document which was then used in court proceedings.

How Organizations Are *Reacting* to Address These Risks

While LATAM countries continue to face increasing cyber threats, organizations in the region are taking steps to address them. This LATAM AppSec Report found LATAM organizations are responding to cybersecurity threats in the following ways:

1. LATAM Organizations Are Increasingly Adopting ***Zero-Trust Strategies***

Zero-Trust strategies are rapidly gaining popularity and becoming essential to digital security measures. These strategies reduce risk by denying access to unauthorized users or systems and requiring authentication for all the resources in the network.

As the rest of the world invested heavily in implementing Zero-Trust strategies, LATAM organizations followed suit. In 2022, many organizations in LATAM adopted Zero-Trust architectures to strengthen application security and reduce the risk of data theft.

2. ***IoT Security*** Is Becoming Increasingly Popular

IoT (Internet of Things) devices are quickly becoming a mainstay in the digital landscape. However, these devices often come with their own unique set of security challenges. LATAM countries have invested heavily in IoT security, with organizations increasingly implementing robust application and device security protocols to secure their IoT devices.

According to **Mordor Intelligence**, the implementation of IoT solutions in Latin American countries, including Mexico, Brazil, and Argentina, has rapidly grown. From optimizing supply chain processes to introducing visibility into healthcare, government offices, and hospitality industries, Wi-Fi networks are optimized with RFID technology, Bluetooth, and sensors for maximum efficiency.

3. LATAM Organizations Are Increasingly ***Investing in Cybersecurity Training***

The success of any cybersecurity strategy depends heavily on the people involved. Therefore, LATAM countries are investing heavily in cybersecurity training and awareness programs to ensure their employees are aware of the latest cyber threats. Organizations in the region are...

...implementing security policies, such as data privacy policies, to ensure the safe management of data.

Finally, organizations are investing in application security solutions and development frameworks to help secure and reduce application vulnerabilities. By investing in security, organizations can ensure that their applications are secure and resilient against cyber threats.

4. ***Application Security*** Through AI and Automation

AI (artificial intelligence) and automation are becoming increasingly popular in LATAM countries as organizations look to reduce application vulnerabilities. AI-based application security tools can detect vulnerabilities before malicious actors exploit them. Similarly, automation can reduce the time spent on application testing and improve the application security process.

5. Increase in ***Cybersecurity Insurance Policies***

Organizations are increasingly investing in cybersecurity insurance policies to protect against the financial loss that cyber-attacks can cause, leading to a greater demand for comprehensive policies.

How LATAM Organizations Can *Prepare* for the Future

As LATAM countries become increasingly vulnerable to cyber threats, organizations in the region must take proactive steps to protect themselves against the latest cyber threats. While most organizations in the region are already taking steps to address these threats, there remains a lot of work to be done. This LATAM AppSec Report provides some tips for LATAM organizations on how to prepare for the future.

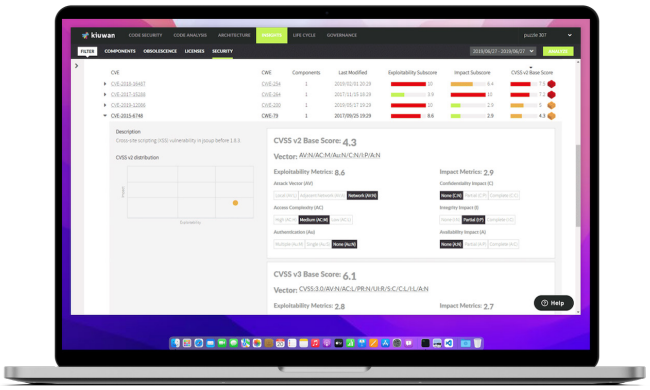
Regular Testing

Regular application testing is a must for organizations to ensure they identify and address application vulnerabilities. There are various tools organizations can use to test application security, such as application penetration testing and source code analysis tools.

Software Composition Analysis (SCA)

Software Composition Analysis is a critical software security tool that can help organizations identify and fix open-source and third-party software code vulnerabilities. SCA works by scanning application code for known vulnerabilities and providing detailed information on how to fix them. SCA can also be used as part of an application security program, helping organizations ensure that application security remains up-to-date and is in line with the latest and best practices.

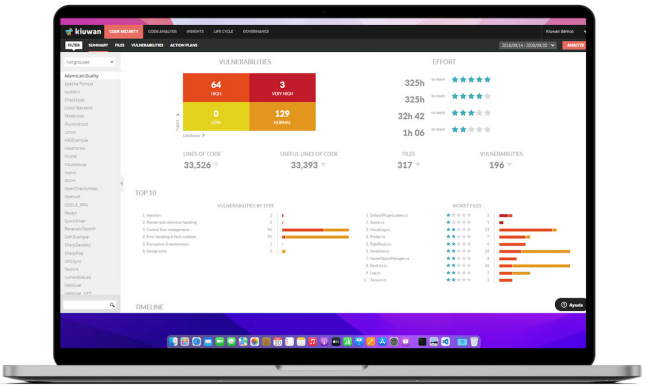
Kiuwan SCA is one of the best solutions organizations in the LATAM region can use to secure their applications. Kiuwan SCA helps organizations identify application vulnerabilities and provides detailed information on how to fix them. The tool integrates seamlessly into existing application development environments and helps organizations quickly produce secure source code. Moreover, Kiuwan Insights provides comprehensive information about open-source code vulnerabilities in source code so that developers can identify and fix them before malicious actors can exploit them.



Static Application Security Testing (SAST)

Static application security testing (SAST) is a critical process that helps organizations identify application vulnerabilities before they release them into production. SAST works by scanning application source code for known development security vulnerabilities. This helps organizations identify application security issues early in development and fix them quickly without breaking builds.

For organizations looking to leverage SAST to protect their application, Kiuwan SAST is one of the best solutions. Kiuwan SAST helps organizations identify all of the application security vulnerabilities in their application source code. The easy-to-use dashboard provides a top-down view of application security issues so developers can visualize and prioritize the application security improvements to make first. The tool also integrates with the organization's DevOps and DevSecOps environment, making application security part of the development process. This also allows developers to address development security vulnerabilities quickly.



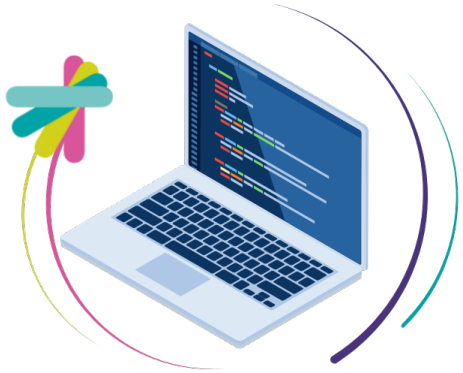
AddOns

AddOns are application security tools designed to help organizations develop more secure applications. They typically provide application-specific protection and can be integrated into existing application development processes. The application security tools offered by AddOns can include application whitelisting, hardening, scanning, and testing.

Kiuwan QA is a valuable addition to application development security due to its multifunctional capabilities, which allow organizations to go beyond just code analysis and create an entire secure ecosystem for their applications. The decision-oriented indicators of Kiuwan support modifications while being directly integrated into the existing infrastructure, requiring no installation. With this powerful tool, organizations can take development security to unprecedented heights by quickly recognizing and solving potential vulnerabilities.

Secure Your Organization's Application Development Process With Kiuwan

Is your organization looking to ensure application security? Kiuwan can help. Our application security solutions provide organizations with the tools they need to build secure applications from the ground up. With Kiuwan, application security becomes part of your development process. Additionally, application vulnerabilities can be identified and fixed quickly, reducing application risk and improving protection.



Contact us today to learn how Kiuwan can help safeguard your application development process from the latest security threats.

*YOU KNOW **CODE**, WE KNOW **SECURITY**!*

GET IN TOUCH:

Headquarters
2950 N Loop Freeway W, Ste 700
Houston, TX 77092, USA

United States **+1 732 895 9870**
Asia-Pacific, Europe, Middle East and Africa **+44 1628 684407**
contact@kiuwan.com
Partnerships: **partners@kiuwan.com**